CLAIMS

What is claimed is:

Sub A1

1. A computerized method for scanning files for viruses comprising:

generating a current session key upon an execution of the method;

obtaining a session stamp associated with a directory entry for a file;

scanning the file if the session stamp was created using a previous session key; and

updating the session stamp as a result of the scan.

2. The method of claim 1, further comprising:

scanning the file if there is no session stamp associated with the directory entry for the file; and

creating a session stamp using the current session key as a result of the scan.

3. The method of claim 1, wherein updating the session stamp comprises invalidating the session stamp if the file is infected with a virus.

4. The method of claim 1, wherein the session stamp comprises an infection indicator and updating the session stamp comprises modifying the infection indicator when the file is infected with a virus.

5. The method of claim 1, wherein the session stamp comprises a signature and updating the session stamp comprises encrypting a known value with the current session key to create the signature.

6. The method of claim 1, wherein the session stamp comprises a signature and updating the session stamp comprises replacing a previous session key with the current session key.

a1

7. The method of claim 1, wherein the session stamp comprises context information and updating the session stamp comprises replacing previous context information with current context information.

8. The method of claim 1, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed when the file is accessed.

9. The method of claim 1, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed upon the file as a result of a user command.

10. The method of claim 1, further comprising:

loading a pre-determined set of file identifiers, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed on each file identified by the file identifiers.

11. The method of claim 10, wherein the pre-determined set of file identifiers is a most-recently-used cache of identifiers for the files that have been most recently used, and further comprising:

adding an identifier for the file to the most-recently-used cache when the file is accessed; and

storing the most-recently-used cache to non-volatile storage upon termination of the execution.

12. The method of claim 10, wherein the pre-determined set of file identifiers is created from user input.

a1

13. The method of claim 10, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed as a background task on each file identified by the file identifiers.

14. The method of claim 1, wherein the session stamp is stored in an extended attributes section of the directory entry for the file.

09761050.011100

15. A computer-readable medium having stored thereon executable instructions to cause a computer to perform a method comprising:

generating a current session key upon an execution of the instructions;

obtaining a session stamp associated with a directory entry for a file;

scanning the file if the session stamp was created using a previous session key; and

updating the session stamp as a result of the scan.

16. The computer-readable medium of claim 15, further comprising:

scanning the file if there is no session stamp associated with the directory entry for the file; and

creating a session stamp using the current session key as a result of the scan.

17. The computer-readable medium of claim 15, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed when the file is accessed.

18. The computer-readable medium of claim 15, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed upon the file as a result of a user command.

a1

19. The computer-readable medium of claim 15, further comprising:

loading a pre-determined set of file identifiers, wherein obtaining the session stamp, scanning the file, and updating the session stamp are performed on each file identified by the file identifier.

20. The computer-readable medium of claim 15, wherein the session stamp is stored in an extended attributes section of the directory entry for the file.

21. A computer-readable medium having stored thereon a session stamp data structure comprising:

a file identifier field containing data representing an identifier for a file in a file system; and

a signature field containing data created by an execution of an anti-virus process that last scanned the file identified by the file identifier field.

22. The computer-readable medium of claim 21, wherein the data in the signature field represents a pre-determined value encrypted by a session key associated with the execution of the anti-virus process.

23. The computer-readable medium of claim 21, wherein the data in the signature field represents a session key associated with the execution of the anti-virus process.

24. The computer-readable medium of claim 21, further comprising:

a scanner settings field containing data representing a configuration for the anti-virus process that last scanned the file identified by the file identifier field.

a1

25. The computer-readable medium of claim 21, further comprising:

a scan result field containing data representing an infection status returned by the anti-virus process that last scanned the file identified by the file identifier field.

26. The computer readable medium of claim 21, further comprising:

a time and date stamp field containing data representing a time and date the file identified by the file identifier field was last modified.

27. The computer-readable medium of claim 21, further comprising:

a size field containing data representing a size for the file identified by the file identifier field.

28. A computer system comprising:

a processor coupled to a system bus;

a memory coupled to the processor through the system bus;

a computer-readable medium coupled to the processor through the system bus;

a virus scanning process executed from the computer-readable medium by the processor, wherein the scanning process causes the processor to generate a current session key when the scanning process is executed from the computer-readable medium, and further to obtain a session stamp associated with a directory entry for a file from the computer-readable medium, to scan the file if the session stamp was created using a previous session key, and to update the session stamp on the computer-readable medium as a result of the scan.

29. The computer system of claim 28, wherein the virus scanning process further causes the processor to scan the file if there is no session stamp associated with the directory entry for the file on the computer-readable medium, to create a session stamp using the current session key as a result of the scan, and to store the session stamp in the directory entry for the file on the computer-readable medium.

a1

30. The computer system of claim 28, further comprising a user input device coupled to the processor through the system bus, wherein input from the user input device instructs the virus scanning process to scan the file.

09481060 .011100

31. The computer system of claim 28, further comprising an application process executed from the computer-readable medium by the process, wherein a request from the application process for the file causes the processor to scan the file.

32. A method for communicating between an anti-virus process and a session stamping process comprising:

issuing, by the anti-virus process, an enable-session-key call;

receiving, by the session stamping process, the enable-session-key call and, in response thereto, initializing a stamping session and generating a session key;

issuing, by the anti-virus process, a disable-session-key call; and

receiving, by the session stamping process, the disable-session-key call and, in response thereto, disabling the stamping session.

33. The method of claim 32, further comprising:

issuing, by the anti-virus process, a stamp-file-with-session-stamp call having a file parameter; and

receiving, by the session stamping process, the stamp-file-with-session-stamp call and, in response thereto, generating a session stamp using the session key and associating the session stamp with a file identified by the file parameter.

a'

34. The method of claim 33, wherein the stamp-file-with-session-stamp call further has an engine parameter identifying context information used to generate the session stamp.

35. The method of claim 33, wherein the stamp-file-with-session-stamp call further has an iam parameter identifying the anti-virus process currently calling the session stamping process.

36. The method of claim 32, further comprising:

issuing, by the anti-virus process, a delete-session-stamp call having a file parameter; and

receiving, by the session stamping process, the delete-session-stamp call and, in response thereto, deleting any session stamp associated with the file identified by the file parameter.

37. The method of claim 32, further comprising:

issuing, by the anti-virus process, a has-file-got-valid-session-stamp call having a file parameter;

receiving, by the session stamping process, the has-file-got-valid-session-stamp call and, in response thereto, determining a validity for any session stamp associated with the file identified by the file parameter; and

returning, by the session stamping process, the validity to the anti-virus process.

38. The method of claim 37, wherein the has-file-got-valid-session-stamp call further has an engine parameter identifying context information used to determine the validity of the session stamp.

39. The method of claim 37, wherein the has-file-got-valid-session-stamp call further has an iam parameter identifying the anti-virus process currently calling the session stamping process.

40. The method of claim 37, wherein the has-file-got-valid-session-stamp call further has a signer parameter, and further comprising:

returning, by the session stamping process, an identifier for the anti-virus process that last called the session stamping process as the signer parameter.